

Department of Justice

§ 23.3

(2) Set out specific purposes in connection with which information will be used;

(3) Limit, where appropriate, the scope of the information subject to such consent.

[41 FR 54846, Dec. 15, 1976, as amended at 45 FR 62038, Sept. 18, 1980]

§ 23.29 Sanctions.

Where BJA, OJJDP, BJS, NIJ, or OJP believes that a violation of section 812(a) of the Act or section 1407(d) of the Victims of Crime Act, these regulations, or any grant or contract conditions entered into thereunder has occurred, it may initiate administrative actions leading to termination of a grant or contract, commence appropriate personnel and/or other procedures in cases involving Federal employees, and/or initiate appropriate legal actions leading to imposition of a civil penalty not to exceed \$10,000 for a violation occurring before September 29, 1999, and not to exceed \$11,000 for a violation occurring on or after September 29, 1999 against any person responsible for such violations.

[Order No. 2249-99, 64 FR 47102, Aug. 30, 1999]

PART 23—CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Sec.

23.1 Purpose.

23.2 Background.

23.3 Applicability.

23.20 Operating principles.

23.30 Funding guidelines.

23.40 Monitoring and auditing of grants for the funding of intelligence systems.

AUTHORITY: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

SOURCE: 58 FR 48452, Sept. 16, 1993, unless otherwise noted.

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L.

100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies:

(1) *Criminal Intelligence System* or *Intelligence System* means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information;

(2) *Interjurisdictional Intelligence System* means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions;

(3) *Criminal Intelligence Information* means data which has been evaluated to determine that it:

(i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization

which is reasonably suspected of involvement in criminal activity, and

(ii) Meets criminal intelligence system submission criteria;

(4) *Participating Agency* means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system;

(5) *Intelligence Project* or *Project* means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and

(6) *Validation of Information* means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) *Reasonable Suspicion* or *Criminal Predicate* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable

possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f)(1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A